UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,889	11/21/2003	Jie Liang	TI-35866	1647

23494 7590 10/10/2008
TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
10/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com

Office Action Summary	Application No.	Applicant(s)	
	10/718,889	LIANG, JIE	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *July 16, 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Response filed on July 16, 2008.

Claiming benefits from Provisional Application, 60/440575, filed on January 16, 2003.

Claims 1-26 are originally pending.

Response to Arguments

1. Applicant's arguments filed July 16, 2008 have been fully considered but they are not persuasive.

IEEE 802.11 (1999) teaches the limitation "suppressing a sequence number input to a message integrity code" [IEEE 802.11 (1999), pg 63 – "the WEP algorithm is applied to the frame body of an MPDU (Fig 12), thus precluding the sequence number. The MIC is inherent in the WEP algorithm.]. To clarify the relationship of the MSDU and the sequence number, Section 9.1.4 describes how data packets, MSDU/MMPDU, are fragmented into MPDUs. From each fragmented piece of a data packet, a MAC header and CRC is generated to form a fragmented "MSDU" called an MPDU. The appropriate Sequence number of a particular MPDU is generated and contained in the Sequence Control Field, [Pg 40, Sec 7.1.3.4.1]. The Sequence Control Field is part of the MAC header [Pg 34, Sec 7.1.2]. The frame body, from which the WEP algorithm is applied, does not contain the sequence number, thus "suppressing a sequence number input to a message integrity code algorithm." Instead of the frame body comprising the MSDU as mischaracterized by the Applicant, Page 34, Sec 7.1.2 states that the MSDU/MPDU/MMPDU actually comprises the frame body. Page 40, Section 7.1.3.5 explains that the maximum length of the frame body field would vary depending on the

size, which is defined by the maximum length (MSDU + ICV + IV). In this case, the MSDU is the plaintext message from which WEP will be applied that make up the frame body.

To further explain the rejection of claim 12, IEEE 802.11 (1999) teaches assigning sequence numbers to all messages in the order of transmission and including the sequence number in each transmitted message [IEEE 802.11 ed. 1999, pg 40], assigning fragment numbers to all messages in the order of fragmentation of each message and including the fragment number in each transmitted message [IEEE 802.11 ed. 1999, pg 40], and including a transmitted message integrity code in each transmitted message [IEEE 802.11 ed. 1999, pg 63]. Jakubowski teaches the part of calculating a message integrity code (or message authentication code) using an encryption process [US 6128737, Abstract] to calculate the transmitted message integrity code. Shu teaches the part of using an encryption process based in part on a fragment number [US 7171493 B2, Col 9, Ln 47-52 --Examiner notes private header reads on fragment number.] to calculate the transmitted message integrity code as taught by Jakubowski. Thus the IEEE 802.11 standard 1999 ed., in view of Shu, and Jakubowski teaches all the limitations of claim 12 as previously cited. It is not persuasive that Jakubowski may not teach or suggest calculating based on the fragment number as argued by the Applicant because Jakubowski teaches a part of using an encryption process to calculate a message integrity code which is the same encryption process that is suggested to be modified in view of Shu.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 1-4, 7-9, 12-16, 19-22, and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the IEEE 802.11 standard 1999 ed., and further in view of Shu et al. [US 7171493 B2], hereinafter Shu, and Jakubowski et al. [US 6128737], hereinafter Jakubowski.

Regarding claim 1, the IEEE 802.11 (1999) teaches a method for generating a message integrity code in a wireless local area network operating under an IEEE 802.11 standard comprising: suppressing a sequence number input to a message integrity code algorithm [IEEE 802.11 (1999), pg 63 --Examiner notes that "the WEP algorithm is applied to the frame body of an MPDU (Fig 12), thus precluding the sequence number. The MIC is inherent in the WEP algorithm.].

The IEEE 802.11 (1999) does not explicitly teach calculating a message integrity code based in part on a fragment number.

Shu teaches using an encryption process based in part on a fragment number [US 7171493 B2, Col 9, Ln 47-52 --Examiner notes private header reads on fragment number.]

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify the IEEE 802.11 (1999) ed. incorporating the private header, such as a fragment number, into an encryption process as taught by Shu. The suggestion/motivation would have been to protect various types of attacks [US 7171493 B2, Col 2, Ln 3-8] that would

have exploited private header information. Shu is an analogous art because it is in the same field of network communication and it solves the problem by providing more security into a communication protocol.

However, the IEEE 802.11 (1999) ed. in view of Shu does not explicitly teach generating a message integrity code using an encryption process.

Jakubowski teaches generating a message integrity code (or message authentication code) using an encryption process [US 6128737, Abstract].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify the IEEE 802.11 (1999) ed. in view of Shu by using an encryption process that generates a message integrity code as taught by Jakubowski. The motivation for combining would have been to provide for a cryptographic technique that provides for both confidentiality and integrity [US 6128737, Col 3, Ln 22-30]. Jakubowski is analogous art because it is in the same field of network communication and it solves the problem by providing more security in a communication protocol.

Regarding claim 2, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 1, wherein the sequence number input is set to all zeros [Official notice is taken that it is common and well known in the art to pad number fields with zeros as an act of suppressing or muting a number field in an algorithm.].

Regarding claim 3, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 1, further comprising assigning a sequence number to each message and assigning packet numbers to message fragments in the order of fragmentation [IEEE 802.11 ed. 1999, pg 40].

Regarding claim 4, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 3, further comprising transmitting the message to a receiving station [IEEE 802.11 ed. 1999, pg 10].

Claims 7 and 8 are rejected because the combined claims are similar matter to claim 1.

Claim 9 is rejected because it is similar matter as claim 2.

Regarding claim 12, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method for providing security for messages transmitted over a wireless local area network, comprising: assigning sequence numbers to all messages in the order of transmission and including the sequence number in each transmitted message [IEEE 802.11 ed. 1999, pg 40], assigning fragment numbers to all messages in the order of fragmentation of each message and including the fragment number in each transmitted message [IEEE 802.11 ed. 1999, pg 40], and calculating a transmitted message integrity code [US 6128737, Abstract] based in part on the fragment number for each transmitted message [US 7171493 B2, Col 9, Ln 47-52 --Examiner notes private header reads on fragment number.] and including the transmitted message integrity code in each transmitted message [IEEE 802.11 ed. 1999, pg 63.].

Regarding claim 13, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 12, further comprising: encrypting the transmitted message integrity code before transmitting each message [IEEE 802.11 ed. 1999, pg 63.].

Regarding claim 14, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 12, further comprising: upon receipt of a message, calculating a received message integrity code [US 6128737, Abstract] based in part on

the fragment number for the received message [US 7171493 B2, Col 9, Ln 47-52 -- Examiner notes private header reads on fragment number.].

Regarding 15, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 14, further comprising: comparing the transmitted message integrity code to the received message integrity code [IEEE 802.11 ed. 1999, pg 64.].

Regarding claim 16, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski method according to Claim 15, further comprising: rejecting the received message if the transmitted message integrity code does not match the received message integrity code [IEEE 802.11 ed. 1999, pg 64.].

Claims 19, 20 are rejected because it is similar matter as claims 1 and 3 respectively.

Claim 21 is rejected because it is similar matter to claims 1 and 14 combined.

Claim 22 is rejected because it is similar matter to claims 15 and 16 combined.

Claim 24 is rejected because it is similar matter to claim 12.

Claim 25 is rejected because it is similar matter to claims 14, 15, and 16 combined.

2. Claims 5-6, 10-11, 17-18, 23, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over the IEEE 802.11 standard 1999 ed., and further in view of Shu et al. [US 7171493 B2], hereinafter Shu, Jakubowski et al. [US 6128737], hereinafter Jakubowski, and Jiang et al. [US 6765885 B2], hereinafter Jiang.

Regarding claim 5, the IEEE 802.11 standard 1999 ed., Shu, and Jakubowski teach a method according to Claim 4. The IEEE 802.11 standard 1999 ed., Shu, and Jakubowski does not explicitly teach further comprising: upon receipt of a plurality of

messages having the same sequence number at a receiving station, and checking the received packet numbers for a complete sequence.

Jiang teaches a determination of acceptable sequence number ranges in a communication protocol comprising: upon receipt of a plurality of messages having a same sequence number at a receiving station [US 6765885 B2, Col 8, Ln 35-37 – Examiner notes preserving PDUs having an expected range of packet numbers read on messages having a same IEEE 802.11 sequence number.], and checking the received packet numbers for a complete sequence [US 6765885 B2, Col 8, Ln 37-43].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify the IEEE 802.11 standard 1999 ed. in view of Shu, and Jakubowski to check received packet numbers for a complete sequence as taught by Jiang. The suggestion/motivation for preserving a complete sequence of packet numbers would have been to preclude corrupted data in a data stream [US 6765885 B2, Col 8, Ln 39-41]. Jiang is analogous art because it solves the problem of eliminating corruption in a communication protocol.

Regarding claim 6, the IEEE 802.11 standard 1999 ed., Shu, Jakubowski, and Jiang teach a method according to Claim 5 further comprising rejecting a message if it does not have a complete sequence of packet numbers [US 6765885 B2, Col 8, Ln 37-43].

Claim 10 is rejected because it is similar matter of claims 3, 4, and 5 combined.

Claim 17 is rejected because it is similar matter to claim 5.

Claims 11, 18 are rejected because it is similar matter to claim 6.

Claim 23 is rejected because it is similar matter to claims 17 and 18 combined.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132